



## Methods Intrusion to Confidentiality in Cyber-Electromagnetic Networks (Case Study of Military Ad-Hoc Network)

Sajad Alimohammadi<sup>1</sup>✉ | Vahid Sajadi Asil<sup>2</sup>

1. Master of Defense Management of AJA Command and Staff University, Tehran, Iran.

E-mail: [s.alimohammadi33@casu.ac.ir](mailto:s.alimohammadi33@casu.ac.ir)

2. . Master of Defense Management of AJA Command and Staff University, Tehran, Iran.

E-mail: [v.d.sajadi@gmail.com](mailto:v.d.sajadi@gmail.com)

### Article Info

#### Article type:

Research Article

#### Article history:

Received

11 July 2024

Received in revised form

10 November 2024

Accepted

9 January 2025

Published online

16 September 2025

#### Keywords:

*Ad hoc network,*

*Confidentiality,*

*Intrusion*

### ABSTRACT

**Objective:** to identify methods of infiltrating military ad-hoc networks from the aspect of confidentiality.

**Methodology:** the type of applied research and the method of this research is descriptive because the researcher seeks to identify the subject and based on what it is and without the intervention and manipulation of variables with the available information regarding the identification of the methods of penetration into cyber electromagnetic networks in a systematic and descriptive manner. Systematically address the current situation, and the research approach is mixed

The statistical population is the employees working in the army of the Islamic Republic of Iran, who are familiar with the concepts of cyber-electromagnetism and have at least 15 years of service in such jobs.

**Findings:** In the field of confidentiality, 9 active classic attacks, 7 passive classic attacks and 5 attack methods were identified based on the attack meter database.

**Conclusion:** Among the attacks, the three indicators of impersonation attack with an average of (4.79), packet injection attack with an average of (4.74), and Sybil attack with an average of (4.67) for the active classic component, the three indicators of traffic analysis attack with an average of (4.81), traffic interception attack with an average of (4.80), and packet sniffing attack with an average of (4.69) for the passive classic component, and the two indicators of remote denial of service attack with an average of (4.88) and WPA/WPA2 crack attack with an average of (4.87) for the meter attack component, according to the statistical community, are the best attacks on the confidentiality of military ad hoc networks.

**Cite this article:** : Alimohammadi, S., Sajadi asil, V. (2025). Methods Intrusion To Confidentiality In Cyber-Electromagnetic Networks (Case Study Of Military Ad-Hoc Network). *military science & tactics*, 21 (72), 125-147.

DOI: <http://doi.org/10.22034/qjmst.2025.2035337.2086>



**Publisher:** AJA Command and Staff University

DOI:10.22034/qjmst.2025.2035337.2086

## شیوه‌های نفوذ به محرمانگی در شبکه‌های سایبرالکترومغناطیس (مورد

### مطالعه شبکه اد\_هاک نظامی)

سجاد علی محمدی<sup>۱</sup> | وحید سجادی اصیل<sup>۲</sup>

۱. کارشناس ارشد مدیریت دفاعی دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: [s.alimohammadi33@casu.ac.ir](mailto:s.alimohammadi33@casu.ac.ir)

۲. کارشناس ارشد مدیریت دفاعی دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: [v.d.sajadi@gmail.com](mailto:v.d.sajadi@gmail.com)

اطلاعات مقاله	چکیده
<b>نوع مقاله:</b> مقاله پژوهشی	<b>هدف:</b> شناسایی شیوه‌های نفوذ به شبکه اد_هاک نظامی از بعد محرمانگی است. <b>روش‌شناسی:</b> این تحقیق از نوع کاربردی با روش توصیفی و رویکرد آمیخته است.
<b>تاریخ دریافت:</b> ۱۴۰۳/۰۴/۲۱	جامعه مورد مطالعه در این تحقیق، کتب، مقالات، اسناد و مدارک موجود و همچنین نظرات اخذ شده در قالب مصاحبه با تعداد ۸ نفر صاحب‌نظرانی که در حوزه شبکه‌های سایبرالکترومغناطیس از دانش کافی برخوردار می‌باشند. جامعه آماری تحقیق ۱۳۰ نفر با مشخصات، آشنایی با شبکه‌های سایبرالکترومغناطیس، شبکه‌های مخابراتی و رایانه‌ای، حداقل دارای مدرک کارشناسی و ۱۰ سال سابقه خدمت باشند بودند که نظرات آن‌ها در قالب پرسشنامه دریافت و مورد تجزیه و تحلیل قرار گرفت.
<b>تاریخ بازنگری:</b> ۱۴۰۳/۰۸/۲۰	<b>یافته‌ها:</b> در حوزه نفوذ به محرمانگی، ۹ حمله کلاسیک فعال، ۷ حمله کلاسیک غیرفعال و ۵ روش حمله بر اساس پایگاه داده میتر اتک شناسایی گردید.
<b>تاریخ پذیرش:</b> ۱۴۰۳/۱۰/۲۰	نتیجه‌گیری: از میان حملات، سه شاخص حمله جعل هویت با میانگین (۴/۷۹)، حمله تزریق بسته با میانگین (۴/۷۴) و حمله سبیل با میانگین (۴/۶۷)، برای مؤلفه کلاسیک فعال، سه شاخص حمله تجزیه و تحلیل ترافیک با میانگین (۴/۸۱)، حمله ره‌گیری ترافیک با میانگین (۴/۸۰) و حمله استشمام بسته با میانگین (۴/۶۹) برای مؤلفه کلاسیک غیرفعال و دو شاخص حمله جلوگیری از سرویس از راه دور با میانگین (۴/۸۸) و حمله کرک دلبلیو پی‌ای/دلبلیو پی‌ای دو با میانگین (۴/۸۷) برای مؤلفه میتر اتک، بر اساس نظر جامعه آماری، بهترین حملات به محرمانگی شبکه‌های اد_هاک نظامی هستند.
<b>تاریخ انتشار:</b> ۱۴۰۴/۰۶/۲۵	
<b>کلیدواژه‌ها:</b> شبکه اد_هاک، محرمانگی، نفوذ.	

**استناد:** علی محمدی، سجاد و سجادی اصیل، وحید. (۱۴۰۳). شیوه‌های نفوذ به محرمانگی در شبکه‌های

سایبرالکترومغناطیس (مورد مطالعه شبکه اد\_هاک نظامی). *علمی علوم و فنون نظامی*، ۲۱ (۷۲)، ۱۴۷-۱۲۵.

DOI: <http://doi.org/10.22034/qjmst.2025.2035337.2086>



DOI: 10.22034/qjmst.2025.2035337.2086

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران



## Methods Intrusion To Confidentiality In Cyber-Electromagnetic Networks (Case Study Of Military Ad-Hoc Network)

Sajad Alimohammadi<sup>1</sup> | Vahid Sajadi Asil<sup>2</sup>

### Extended Abstract

#### Introduction

In recent years, the convergence of electronic warfare and cyber warfare has emerged as a central theme in international discussions. Since 2014, the U.S. military has been actively integrating these two domains and has published new guidelines. This research explores methods for breaching confidentiality in ad-hoc networks, which are utilized temporarily and without infrastructure. These networks exhibit characteristics such as security, resilience, and rapid deployability due to their independence from fixed infrastructures. The security challenges of ad-hoc networks encompass availability, integrity, confidentiality, and authentication. Security attacks can be broadly classified into active and passive types and may stem from external actors or internal nodes. Furthermore, various encryption techniques and strategies are available to safeguard confidentiality. Different attacks that threaten confidentiality include traffic analysis, man-in-the-middle attacks, and cellular network spoofing. Given the importance of messages in military networks, identifying the most effective penetration methods to uphold security and enhance the efficiency of these networks is crucial. Various studies have investigated ad-hoc networks and their security, particularly in military and wireless domains. Shamsavari (2013) discussed the advantages and characteristics of ad-hoc networks along with their security challenges. Mohammadi (2020) examined the security of Wi-Fi protocols, addressing existing issues in older protocols, while Afshar Herati (2021) focused on new security features in ad-hoc networks. Sbai and Elboukhari (2018) and Chang et al. (2018) explored various classical attacks on these networks. Abousaleh et al. (2008) also highlighted the risks of identity spoofing attacks in routing protocols. The present research places greater emphasis on methods of compromising confidentiality in ad-hoc networks and utilizes classical attacks alongside a metric attack database.

#### Methodology

This study was conducted descriptively, employing both qualitative and quantitative data. The target population comprised scientific articles, books, and expert opinions, while data collection tools included interviews and questionnaires. Data analysis was performed using Atlas Ti and Smart PLS software, and the results of Cronbach's alpha test indicate acceptable reliability of the measurement model.

#### Findings

Additionally, the variance inflation factor was calculated to evaluate multicollinearity among variables. This research identified methods for infiltrating ad-hoc networks. By employing descriptive methods and tools such as documents and interviews, the findings were derived from both qualitative and quantitative analyses. The results indicate an increasing use of ad-hoc networks, particularly within military organizations.

#### Conclusion

This research was conducted to identify methods of intrusion into ad-hoc networks. A descriptive method with a mixed approach was employed in this study, utilizing tools such as documents, interviews, and questionnaires for data collection. To achieve the main objective of the research, past research sources, books, existing documents, and interviews with experts aligned with the research goals were qualitatively analyzed using Atlas Ti software. Based on the results obtained, a



questionnaire was developed and sent to the sample group for responses. After collection, the data were quantitatively analyzed (descriptively) using SPSS and Smart PLS software. The overall summary of the final results, based on the research questions, is presented below.

Considering the findings of the research, it can be concluded that the use of ad-hoc networks is increasing due to their ease and speed of deployment, high mobility, and dynamic topology. One of the areas where the use of this network is on the rise is military organizations, several examples of which are mentioned in the theoretical framework section. Hermes Company, as a major provider of military wireless systems, is capable of utilizing ad-hoc networks. This study aimed to ensure maximum accuracy in selecting intrusion methods suitable for military ad-hoc networks, relying on credible sources and expert opinions. The results for intruding into confidentiality are detailed below. Confidentiality, as previously stated, refers to the protection of data transmitted by a device in such a way that it becomes unreadable by an unauthorized individual or access point. Since wireless networks broadcast in all directions and fall within the range of direct data transmission, they facilitate data retrieval and eavesdropping, making it crucial to keep data confidential from unauthorized users or devices. Currently, there are many methods employed to maintain confidentiality in ad-hoc networks, which somewhat complicate unauthorized access.

The most significant intrusion techniques in ad-hoc networks concerning confidentiality, based on the analysis conducted, include:

- Classic active attacks, comprising identity spoofing, packet injection, man-in-the-middle attacks, cellular network spoofing, and denial-of-service attacks;
- Classic passive attacks, including traffic analysis, traffic interception, packet sniffing, packet extraction, and information leakage;
- MitM attacks, which include remote service denial attacks and WPA/WPA2 cracking attacks.

## مقدمه

در چند سال اخیر، نشست‌های بین‌المللی زیادی با محوریت همگرایی جنگ الکترونیک و جنگ سایبر در راستای، نقش و اهمیت همگرایی بین جنگ الکترونیک و جنگ سایبری در حال برگزاری است. از سال ۲۰۱۴ ارتش آمریکا به‌صورت جدی و عملیاتی، همگرایی جنگ الکترونیک و جنگ سایبری را مورد توجه قرار داده و در این راستا دستورالعمل اجرایی اف-ام ۳۸-۳ را با عنوان «فعالیت‌های سایبر الکترومغناطیس» منتشر نمود. در آوریل سال ۲۰۲۱، دستورالعمل اجرایی اف-ام ۱۲-۳ با موضوع «عملیات فضای سایبری و جنگ الکترونیک» به‌عنوان نسخه کامل‌تر، جایگزین اف-ام ۳۸-۳ گردید که در آن تاکتیک‌ها و فرآیندهای هماهنگی و ادغام عملیات فضای سایبر و جنگ الکترونیک نیروی زمینی ارتش آمریکا مشترک ارائه گردید. (فرح بخت، احمدرضا و دهقانی، مهدی. ۱۳۹۸)

از لحاظ تاریخی، شبکه‌های اد-هاک عمدتاً برای برنامه‌های تاکتیکی مرتبط با شبکه، جهت بهبود ارتباطات میدان جنگ استفاده می‌شوند. ماهیت پویای عملیات نظامی باعث می‌شود که نتوان به یک زیرساخت ارتباطی ثابت از قبل پیش‌بینی شده، در میدان نبرد تکیه کرد و همچنین ارتباطات بی‌سیم خالص نیز دارای این محدودیت است که سیگنال‌های رادیویی در معرض تداخل هستند و فرکانس‌های رادیویی بالاتر از ۱۰۰ مگاهرتز به‌ندرت فراتر از خط دید<sup>۱</sup> منتشر می‌شوند. یک شبکه اد-هاک چارچوب مناسبی را برای رسیدگی به این مسائل ایجاد می‌کند، زیرا یک شبکه توزیع‌شده بی‌سیم همراه، بدون نیاز به زیرساخت‌های از پیش تعیین‌شده را ارائه کرده و اتصالاتی فراتر از خط دید مستقیم را فراهم می‌کند (Soni, 2017).

بررسی مطالعات انجام‌شده در خصوص مشخصات و چگونگی بهره‌برداری از این شبکه‌ها، نشان می‌دهد که حوزه امنیتی

شبکه‌های اد-هاک، یکی از مهم‌ترین حوزه‌های متناسب با موضوع تحقیق است؛<sup>۲</sup> و با توجه به مطالعات انجام‌شده پیشین، این پژوهش روش‌های نفوذ به شبکه‌های اد-هاک در حوزه محرمانگی را به‌عنوان یکی از مصادیق شبکه‌های سایبر الکترومغناطیس در بعد امنیتی مورد مطالعه قرار دهد.

<sup>۱</sup> Line Of Side (LOS)

<sup>۲</sup> از جمله این مطالعات می‌توان به مقاله کهیزی، مهدی و همکاران (۱۳۹۳) تحت عنوان چالش‌های امنیتی شبکه‌های کامپیوتری اقتصادی و نیز شرما، شیوی و همکاران (۲۰۱۵) با عنوان الزامات فنی و امنیتی شامل، مسائل، تهدیدات و چالش‌های شبکه اد-هاک اشاره کرد.

محقق قصد دارد در این پژوهش، شیوه‌های نفوذ به محرمانگی در شبکه‌های اد\_هاک را با بهره‌گیری از نظر صاحب‌نظران این حوزه، بررسی نماید.

### مبانی نظری و پیشینه‌های پژوهش

شبکه اد\_هاک بی‌سیم مجموعه‌ای از دستگاه‌هایی است که به‌تنهایی یک شبکه را ایجاد می‌کنند. اد\_هاک اصطلاحی است که برای توصیف اقداماتی که به‌سرعت انجام‌شده یا فقط به‌طور موقت راه‌اندازی می‌گردند، استفاده می‌شود. به علت وجود حالت موقت بدون شبکه می‌توان با استفاده از نقطه دسترسی وای\_فای یا مسیریاب، یک اتصال بی‌سیم به رایانه یا دستگاه دیگری برقرار کرد. اتصالات موقت همچنین می‌تواند منجر به شبکه‌های نظیر به نظیر غیرمتمرکز شود که به طراحی شبکه قبلی متکی نباشند. برخلاف معماری سنتی شبکه که در آن داده‌ها می‌بایست قبل از اینکه به دستگاه‌های گیرنده برسند، به‌طور پیوسته به یک دستگاه مرکزی مانند یک مسیریاب جریان می‌یابند، در شبکه اد\_هاک، هر گره با گره دیگری (مانند تلفن‌ها و رایانه‌های شخصی) می‌تواند به‌طور مستقیم ارتباط برقرار کند (Agrawal, et al., 2023).

شبکه‌های اد\_هاک متحرک نظامی یا تاکتیکی توسط واحدهای نظامی با تأکید بر نرخ داده، نیاز به حداقل تأخیر در استقرار و سرعت در ارسال و برقراری ارتباط، مسیریابی مجدد در حین تحرک، امنیت داده‌ها، برد رادیویی و ادغام با دستگاه‌های موجود مورد استفاده قرار می‌گیرند (Toh, Lee, & Ramos, 2004). شبکه‌های موقت نظامی استقرار سریع، بدون زیرساخت، عدم تماس با دکل‌های رادیویی ثابت، استحکام، امنیت و عملیات فوری را ارائه می‌دهند. شبکه‌های تاکتیکی می‌توانند در طول یک مأموریت تشکیل شوند و پس از پایان مأموریت از راه موبایل، وسیله نقلیه هوایی بدون سرنشین نیروی هوایی<sup>۱</sup>، کشتی نیروی دریایی یا ربات ناپدید گردند (Nabben & Rennie, 2022).

شبکه‌های سلولی شبکه‌هایی هستند که مبتنی بر زیرساخت ثابت هستند. در شبکه سلولی، ارتباط با پیوند بی‌سیم تک‌هاپ انجام می‌شود. این شبکه‌ها اساساً برای ترافیک صوتی طراحی شده‌اند که در آن پهنای باند تضمینی ارائه می‌شود. این بر اساس مسیریابی متمرکز است که در آن پیام با استفاده از سوئیچینگ مدار حرکت می‌کند. شبکه تلفن همراه دارای اتصال یکپارچه است. از این‌رو، کاهش تماس در طول انتقال وجود دارد. عیب اصلی شبکه‌های سلولی این است که زمان بیشتری را برای استقرار مصرف می‌کنند و همچنین نیاز به هزینه

<sup>1</sup> Unmanned Aerial Vehicle (UAV)

بالایی دارند. شبکه اد\_هاک شبکه‌های بدون زیرساخت است که در آن گره‌ها با استفاده از پیوند بی‌سیم به روش چند هاپ ارتباط برقرار می‌کنند. در شبکه اد\_هاک مفهوم مسیریابی توزیع‌شده پیاده‌سازی می‌شود. سوئیچینگ بسته در مقایسه با سوئیچینگ مدار که در شبکه سلولی ترجیح داده می‌شود، حالت ارجح ارتباطی است. گره‌های انتقال، متحرک هستند و برد کمی دارند که منجر به شکست مکرر پیوند می‌شود. مزیت اصلی شبکه اد\_هاک نسبت به شبکه سلولی این است که مستلزم زمان کمتر و هزینه کمتر برای استقرار است (Singh, Dutta, & Chakrabarti, 2018).

### اهمیت فعالیت‌های سایبر الکترومغناطیس در عملیات نظامی

فرماندهان سپاه و لشکر نبردهای دفاعی خود را از طریق جمع‌آوری اطلاعات، آتش‌های مشترک و فعالیت‌های الکترومغناطیسی فضای سایبری<sup>۱</sup> قبل از رسیدن دشمن به منطقه نبرد اصلی<sup>۲</sup> شکل می‌دهند. عملیات فضای سایبری تدافعی<sup>۳</sup> ویژه تهدیدات است و مأموریت برای حفظ توانایی استفاده از شبکه اطلاعات وزارت دفاع<sup>۴</sup> در اولویت قرار دارد. ستاد فرماندهی سپاه و لشکر بر ایجاد اختلال در نیروهای مهاجم قبل از برخورد با منطقه اصلی نبرد و از بین بردن یکپارچگی حمله آن‌ها متمرکز است. فرماندهان سپاه توجه ویژه‌ای به ایجاد اختلال در عناصر فرماندهی و کنترل دشمن از طریق استفاده از اثرات کشنده و غیر کشنده دارند، با این هدف که نیروهای دشمن را در برابر حملات متقابل سپاه و لشکر و حملات خرابکارانه آسیب‌پذیرتر کنند (FM 3-0, OPERATIONS, 2017).

فعالیت‌های الکترومغناطیسی فضای سایبری فرآیند برنامه‌ریزی، یکپارچه‌سازی و همگام‌سازی فضای سایبری و عملیات جنگ الکترونیک در حمایت از عملیات زمینی یکپارچه است. ترکیب فعالیت‌های الکترومغناطیسی فضای سایبری در تمام مراحل یک عملیات کلیدی برای به دست آوردن و حفظ آزادی مانور در فضای سایبری و طیف الکترومغناطیس و درعین حال انکار آن برای دشمنان است. فعالیت‌های الکترومغناطیسی فضای سایبری، قابلیت‌ها را در سراسر حوزه‌ها و عملکردهای جنگی هماهنگ می‌کند و اثرات مکمل را در فضای سایبری و طیف الکترومغناطیس به حداکثر می‌رساند. عملیات‌های اطلاعاتی، سیگنالی، فضای سایبری، فضا و عملیات آتش‌سوزی برای برنامه‌ریزی، همگام‌سازی و اجرای عملیات فضای سایبری و جنگ الکترونیک حیاتی هستند (FM 3-0, OPERATIONS, 2017).

<sup>1</sup> Cyber Electromagnetic Activities (CEMA)

<sup>2</sup> Main Battle Area (MBA)

<sup>3</sup> Defensive Cyberspace Operations (DCO)

<sup>4</sup> Department Of Defense Information Network (DODIN)

مرکز شبکه تاکتیکی مشترک<sup>۱</sup> (جی تی ان سی) در سال ۱۹۹۷، توسط پنتاگون برای برنامه سیستم مشترک رادیویی تاکتیکی با چشم‌انداز اتحاد دستگاه‌های ارتباطی راه‌اندازی گردید. جی تی ان سی به‌عنوان یک منبع واحد برای معماری سیستم‌های باز، کد نرم‌افزار و سایر اطلاعات مرتبط برای دولت و توسعه‌دهندگان نرم‌افزار ارتباطی مورد تأیید، عمل می‌کند (Stukova & Crawford, 2019).

### رادیوهای تاکتیکی مدرن بر پایه شبکه‌های اد\_هاک

شرکت‌هایی مانند AT Communications، Harris Corporation و Persistent Systems شرکای پیشرو در صنعت هستند که سیستم‌های ارتباطی را بر مبنای شبکه‌های اد\_هاک توسعه می‌دهند. رادیو دستی چندکاناله Harris AN/PRC163 یکی از محصولات متعدد آن‌هاست که توسط ارتش برخی کشورها برای تبادل داده بین اپراتورها و مراکز فرماندهی و در سراسر میدان جنگ استفاده می‌شود. این رادیو از فناوری وی اچ اف/یو اچ اف دیدمستقیم، ارتباط ماهواره‌ای و شبکه‌های موقت سیار برای ارسال داده، صدا و تصویر، پشتیبانی می‌کند (Harris Corporation, 2024).

### چالش‌های امنیتی در شبکه‌های موقت بی‌سیم

قبل از تشریح حملات امنیتی و اقدامات متقابل موجود برای انواع مختلف شبکه‌های اد\_هاک، به‌طور خلاصه الزامات اصلی را که معمولاً باید در شبکه‌های اد\_هاک بی‌سیم برآورده شوند، بیان می‌شود:

- ۱- در دسترس بودن: خدمات ارائه‌شده باید به‌موقع در دسترس باشد حتی در صورت وجود مشکل در سیستم. مهم است که خدمات ارائه‌شده توسط شبکه حتی در هنگام حمله در دسترس باشد. هدف حملات کاهش منابع، از بین بردن این ویژگی است.
- ۲- یکپارچگی: اطلاعات ردوبدل شده بین گره‌ها نباید به‌صورت عمدی و سهوی تغییر داده شده باشند؛ بنابراین، برای یک گره مخرب نباید امکان تغییر پیامی که توسط یک گره قانونی ارسال شده است وجود داشته باشد.
- ۳- محرمانگی: اطلاعات طبقه‌بندی‌شده ردوبدل شده در شبکه نباید در اختیار اشخاص غیرمجاز قرار گیرد. محرمانگی را می‌توان با استفاده از چندین فن رمزگذاری انجام داد تا فقط گره‌های قانونی بتوانند محتوای یک بسته را درک کنند. در برخی موارد، مهم است که حتی وجود ارتباط بین دونقطه پایانی را پنهان کنید.

<sup>1</sup> Joint Tactical Networking Center (JTNC)

۴- مجوز: فقط گره‌های مجاز باید بتوانند به شبکه دسترسی داشته باشند و فقط نهادهای مجاز باید بتوانند از خدمات ارائه‌شده توسط شبکه استفاده کنند.

۵- احراز هویت: باید تأیید شود که داده‌ها واقعاً توسط فرستنده ادعا شده ارسال شده است. به این ترتیب، مهاجم نمی‌تواند پیامی را جعل کند و شبکه را وادار کند که پیام ارسالی قانونی است.

۶- انکار: فرستنده نباید بتواند وانمود کند که اطلاعاتی را که واقعاً ارسال کرده است ارسال نکرده است. این ویژگی برای یافتن و جداسازی گره‌های در معرض خطر در شبکه ارزشمند است.

۷- تازگی: داده‌ها باید به گونه‌ای تازه باشند که دشمن نتواند از پیام‌های قدیمی برای گمراه کردن سرویس‌های شبکه از آن‌ها استفاده مجدد کند (Basagni, Conti, Giordano, & Stojmenovic, 2013).

#### طبقه‌بندی حملات امنیتی کلاسیک به شبکه‌های اد\_هاک

حملات کلاسیک علیه شبکه‌های اد\_هاک را می‌توان بر اساس دو طبقه‌بندی کلی تقسیم‌بندی کرد، اولین طبقه‌بندی شامل حملات غیرفعال و فعال است؛ درحالی‌که هدف حملات غیرفعال نظارت و تجزیه و تحلیل رفتار شبکه بدون تداخل با آن است، حملات فعال رفتار عادی شبکه را تغییر می‌دهند.

دومین طبقه‌بندی حملات را می‌توان با در نظر گرفتن عضویت مهاجم در شبکه انجام داد: می‌توان بین حملاتی که توسط یک خارجی و حملاتی که توسط یک گره داخلی سرچشمه می‌گیرند تمایز قائل شود. اولی حملاتی هستند که توسط موجودیت‌هایی ایجاد می‌شوند که به شبکه تعلق ندارند اما می‌خواهند سرویس ارائه‌شده را مختل کنند، درحالی‌که دومی زمانی رخ می‌دهد که گره‌های قانونی به روشی مخرب رفتار کنند (Barmanroy & Chaki, 2014).

#### میترا تک

پایگاه داده میترا تک (تکنیک‌ها، تاکتیک‌ها و دانش مشترک) در سال ۲۰۱۳ برای جمع‌آوری یک ماتریس ساختاری از تکنیک‌های مورداستفاده توسط مجرمان سایبری برای ساده‌سازی کار واکنش به حوادث سایبری ایجاد شد (Enterprise Matrix, 2020).

ATT&CK مخفف عبارت Adversarial Tactics, Techniques, and Common Knowledge است:

- A: متخاصم، مانند یک دولت ملی یا سازمان جنایی
- TT: تاکتیک‌ها و تکنیک‌ها، روش مورد استفاده برای تجزیه و تحلیل حملات سایبری
- CK: دانش مشترک، مستندسازی تکنیک‌ها و تاکتیک‌ها در قالب یک ماتریس

شرکت میترا یک سازمان غیرانتفاعی آمریکایی است که مراکز تحقیق و توسعه با بودجه فدرال را مدیریت می‌کند که از سازمان‌های دولتی ایالات متحده حمایت می‌کنند. (Copeland, 2021, p. 214)

### حملات اخلاص در محرمانگی

حملات علیه حریم خصوصی و محرمانگی حملاتی هستند که سعی در به دست آوردن بینش در مورد داده‌های مبادله شده در شبکه و توپولوژی شبکه را دارند.

یک حریف می‌تواند تجزیه و تحلیل ترافیک را بر روی متن رمز شنیده شده انجام دهد تا اطلاعات مهمی در مورد توپولوژی شبکه و رویدادهای به دست آورد. در مرحله دوم، حریف می‌تواند حملات هدفمندی را اجرا کند تا بخش‌هایی از شبکه را که برای بیشترین تأثیر انتخاب شده است، مختل کند (Basagni, Conti, Giordano, & Stojmenovic, 2013).

در محرمانگی، اطلاعات طبقه‌بندی شده و ردوبدل شده در شبکه نباید در اختیار اشخاص غیرمجاز قرار گیرد. محرمانگی را می‌توان با استفاده از چندین تکنیک رمزگذاری انجام داد تا فقط گره‌های قانونی بتوانند محتوای یک بسته را درک کنند. در برخی موارد، مهم است که حتی وجود ارتباط بین دو نقطه پایانی را پنهان کنید. (Basagni, Conti, Giordano, & Stojmenovic, 2013).

به طبع در شبکه‌های ادهاک نظامی به دلیل اهمیت بالای پیام‌ها از شگردهای امنیتی متفاوتی جهت بالا بردن امنیت در آن‌ها استفاده می‌شود لذا می‌بایست مهم‌ترین شیوه‌ها را شناسایی تا در کمترین زمان ممکن بتوان در این شبکه‌ها نفوذ و از آن‌ها بهره‌برداری نمود.

از دیدگاه صاحب‌نظران، مهاجم از حمله نشست اطلاعات در ارتباطات برای به دست آوردن بینشی در مورد محتوای داده‌ها استفاده می‌کنند؛ با استفاده از حملات مرد میانی، مهاجم بی‌سروصدا ارتباط بین گره‌ها را ره‌گیری و رله می‌کنند؛ با حملات همبستگی ترافیک، مهاجم الگوهای موجود در ترافیک رمزگذاری شده را برای استنباط اطلاعات در مورد طرف‌های ارتباطی مرتبط می‌کنند؛ در حملات بازپخش، مهاجم برای فریب شبکه، بسته‌های داده را ضبط و دوباره ارسال می‌کنند که به‌طور بالقوه منجر به پذیرش داده‌های غیرمجاز یا قدیمی می‌شود؛ با جعل شبکه سلولی، مهاجم شبکه‌های سلولی جعلی ایجاد می‌کند، دستگاه‌های تلفن همراه را از شبکه‌های قانونی منحرف می‌کند و محرمانه بودن داده‌ها را به خطر می‌اندازد؛ از نقاط ضعف پروتکل رمزگذاری دلیو ای پی برای رمزگشایی ترافیک بی‌سیم استفاده می‌کند؛ در حمله از راه دور، هکر با استفاده از ضعف‌های امنیتی در سیستم‌ها و سرویس‌های شبکه، به راه دور وارد آن‌ها می‌شود و اقدام به دسترسی به اطلاعات محرمانه می‌کند و در حمله دوقلوی شیطان‌ی یک

اکسس پوینت جعلی با نامی مشابه با نام قانونی ایجاد می‌کند و مشتریان را فریب می‌دهد تا داده‌هایشان را به هم متصل کرده و افشا کنند.

### پیشینه‌های پژوهش

شاهسوند، محمد (۱۳۹۲) در پایان‌نامه خود با موضوع "شبکه اد\_هاک" به بررسی ویژگی‌ها و اهمیت شبکه اد\_هاک پرداخته و به این نتیجه رسیده است که علی‌رغم مشکلات امنیتی که این شبکه‌ها دارند کاربردهای زیادی نیز دارا هستند؛ در واقع روزبه‌روز بر کارایی آن‌ها افزوده شده است. در این تحقیق، محقق به بررسی ویژگی‌های شبکه‌های اد\_هاک و روش‌های امنیتی بکار گرفته‌شده در شبکه‌های اد\_هاک پرداخته است که از بعد شناسایی موارد امنیتی این شبکه‌ها با تحقیق حاضر دارای اشتراک است. همچنین محقق به دنبال بررسی ویژگی‌ها و اهمیت شبکه اد\_هاک و مزایای آن نسبت به سایر شبکه‌های ارتباطی و مسائل مربوط به امنیت و مسیریابی شبکه‌های اد\_هاک می‌پردازد.

محمدی، حمیدرضا، (۱۳۹۹) در مقاله خود تحت عنوان "بررسی روش‌های نفوذ در شبکه‌های بی‌سیم وای فای" به بررسی امنیت پروتکل‌های شبکه‌های بی‌سیم وای فای پرداخته و به این نتیجه رسیده است که با پروتکل رمزنگاری دلیوای پی و دلیوپی‌ای-دلیوپی‌ای ۲ پرداخته که این پروتکل‌ها قسمت عمده‌ای از ارتباطات خانگی و سازمانی را در ارتباطات بی‌سیم انجام می‌دهند، با ارائه دلیوپی‌ای ۳ کلیه این ایرادات و مشکلات امنیتی رفع شده است؛ اما تجهیزات مجهز به این نوع رمزنگاری در ایران به تعداد کمتری وجود دارند که طبق مطالعات انجام‌شده پروتکل دلیوای پی در بهره‌برداری از آسیب‌پذیری رتبه نخست را دارد و پس از آن پروتکل‌های دلیوپی‌ای نسخه نخست و دوم در رتبه‌های بعدی هستند. در این تحقیق، محقق به بررسی روش‌های نفوذ در شبکه‌های بی‌سیم در خصوص ویژگی یکپارچگی داده‌ها پرداخته که این بعد نقطه اشتراک با این تحقیق است. وجه افتراق این تحقیق با پژوهش حاضر به بررسی فقط در شبکه‌های بی‌سیم وای فای با پروتکل رمزنگاری دلیوای پی و دلیوپی‌ای-دلیوپی‌ای ۲ پرداخته و به اصول اشاره نداشته است.

افشار هراتی، نسرين (۱۴۰۰) در مقاله خود با عنوان "بررسی ساختارهای امنیت در شبکه‌های اد\_هاک با رویکرد نو" به این نتیجه رسیده است که استفاده از ساختار اد\_هاک باعث معرفی برخی ویژگی‌های جدید امنیتی شده است که این ویژگی‌ها در شبکه‌های متداول و مبتنی بر زیرساخت مطرح نشده بودند. این ویژگی‌ها می‌توانند هم به‌صورت نیازها و چالش‌های امنیتی جدید باشند و هم می‌توانند به‌صورت یک مزیت مطرح شوند که از آن برای ایجاد امنیت در شبکه استفاده شود. استفاده گسترده از شبکه‌های اد\_هاک در محیط‌های نظامی و دیگر کاربردهای حساس به امنیت، امنیت را به‌عنوان یک نیاز اساسی از زمان معرفی این شبکه‌ها

مطرح نموده است. در کنار این نیاز، ایجاد امنیت در این دسته از شبکه‌ها مشکلات مخصوص به خود را دارد. در این تحقیق، محقق به بررسی ساختارهای امنیت در شبکه‌های اد\_هاک می‌پردازد و برخی از ویژگی‌های امنیتی این شبکه‌ها را معرفی می‌کند که از این نظر دارای اشتراک با تحقیق حاضر است. این تحقیق تنها به بیان ساختار امنیت در شبکه‌های اد\_هاک در بعد دسترسی‌پذیری می‌پردازد و به روش‌های نفوذ نپرداخته است.

اوساما سبای و محمد البوخاری (۲۰۱۸) در مقاله خود تحت عنوان "طبقه‌بندی حملات شبکه‌های اد\_هاک تلفن همراه" به بررسی انواع حملات کلاسیک در شبکه اد\_هاک پرداخته و یک حمله استراق سمع در لایه شبکه و تجزیه و تحلیل ترافیک در لایه فیزیکی را با عنوان حمله غیرفعال در شبکه اد\_هاک نام برده‌اند. (Sbai & Elboukhari, 2018, p. 618)

تینهو چانگ و همکاران (۲۰۱۸) در مقاله خود با عنوان "روش گرفتن بسته‌های رمز رمزگذاری شده WPA و WPA2، خودکار، نیمه خودکار یا دستی؟" به بررسی موارد امنیتی در شبکه اد\_هاک پرداخته و به سه حمله کلاسیک غیرفعال شامل نظارت و استراق سمع، استتار دشمنان و تجزیه و تحلیل ترافیک اشاره نموده‌اند (Chang, Lin, Chen, & Lai, 2018, p. 2).

ابوساله، خوشار و گویزانی (۲۰۰۸) در مقاله خود تحت عنوان "بررسی پروتکل‌های مسیریابی Ad Hoc ایمن موبایل" به بررسی انواع پروتکل‌های مسیریابی پرداخته و حمله جعل هویت را برجسته نموده است و بیان می‌کند که خطری برای امنیت شبکه تلفن همراه اختصاصی ایجاد می‌کند، به‌ویژه اگر روش احراز هویت صحیح بین گره‌ها وجود نداشته باشد. این حمله می‌تواند به گره‌های مضر اجازه ورود به شبکه و انجام فعالیت‌های نادرست را بدهد که به‌طور بالقوه محرمانگی شبکه را به خطر می‌اندازد (Abusalah, Khokhar, & Guizani, 2008).

وجه افتراق تحقیقات بالا با پژوهش حاضر در این است که در این پژوهش از بعد امنیتی با تأکید بر اصل محرمانگی و بر اساس دو مؤلفه حملات کلاسیک و پایگاه داده میتر اتک، به روش‌های نفوذ به شبکه‌های اد\_هاک پرداخته شد است.

در این تحقیق به شناسایی شیوه‌های نفوذ به محرمانگی در شبکه‌های اد\_هاک بر اساس دو مؤلفه حملات کلاسیک و پایگاه داده میتر اتک، به‌عنوان جنبه نوآوری پرداخته شده است. (بخش‌های قرمز حذف شود)

### روش‌شناسی پژوهش

از آنجاکه محقق به دنبال یافتن پاسخی برای شیوه‌های نفوذ به شبکه‌های سایبر الکترومغناطیس (مورد مطالعه، اد\_هاک نظامی) در حوزه محرمانگی است و در نهایت با ارائه نتایج و پیشنهادهایی که سودمندی علمی را داشته باشد منجر به یافتن راه‌های نفوذ و روش‌های مقابله با آن شود، بنابراین نوع تحقیق کاربردی است.

روش تحقیق، توصیفی است؛ زیرا محقق به دنبال شناسایی موضوع بوده و بر اساس آنچه هست و بدون دخالت و دست‌کاری متغیرها در خصوص شناسایی شیوه‌های نفوذ به محرمانگی به توصیف منظم و نظام‌مند حملات می‌پردازند.

با توجه به اینکه محقق داده‌های به‌دست‌آمده و شواهد خود را درباره پدیده، مطالعه نموده و ابتدا از طریق گردآوری و تحلیل کیفی داده‌ها با نرم‌افزار اطلس تی‌ای فرایند را تکمیل کرده و پس از تحلیل داده‌های به‌دست‌آمده از طریق تحلیل کمی با نرم‌افزار اس‌پی‌اس‌اس و اسمارت پی‌ال‌اس به تلفیق دو روش پرداخته است؛ پس رویکر تحقیق آمیخته است.

در این پژوهش جامعه مورد مطالعه، مقالات علمی معتبر، کتب مرتبط با موضوع، اسناد و مدارک موجود و همچنین استفاده از نظرات دریافت شده از مصاحبه با تعداد ۷ نفر صاحب‌نظران و خبرگانی است که در حوزه شبکه‌های سایبر الکترومغناطیس، دانش کافی را دارا بوده و به‌صورت عملی نیز در حال فعالیت در این حوزه می‌باشند. جامعه آماری، مرحله کمی، ۱۳۰ نفر با ویژگی‌های، آشنایی با شبکه‌های سایبر الکترومغناطیس، آشنایی با شبکه‌های مخابراتی و رایانه‌ای، حداقل دارای مدرک کارشناسی و ۱۰ سال سابقه خدمت باشند، بودند که نظرات آن‌ها در قالب پرسشنامه دریافت و مورد تجزیه و تحلیل قرار گرفت. روش نمونه‌گیری به‌صورت تصادفی ساده<sup>۱</sup> بوده و جامعه نمونه با فرمول کوکران با سطح خطای ۵ درصد، برابر ۹۷ نفر است.

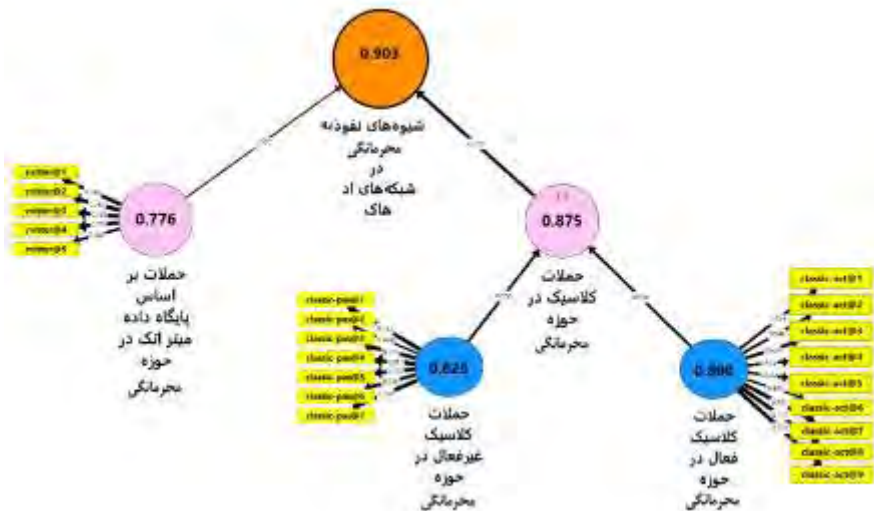
ابزارهای گردآوری اطلاعات به‌صورت میدانی و کتابخانه‌ای بوده و در روش میدانی از ابزار مصاحبه و پرسش‌نامه استفاده گردیده است.

در این تحقیق، تجزیه و تحلیل داده‌های کیفی با استفاده از روش تحلیل محتوا با استفاده از نرم‌افزار اطلس تی‌ای نسخه ۸،۴ و به شرح زیر انجام پذیرفته است:

برای انجام تحلیل کیفی در نرم‌افزار اطلس تی‌ای، در ابتدا پیشینه تحقیق و مصاحبه‌های صورت گرفته به‌صورت مجزا با عنوان سند تفکیک گردید. در گام دوم، پردازش اطلاعات شامل همگرایی داده‌ها (ترکیب)، واگرایی (تعدیل) و تقارن که از مجموع دسته‌بندی با تخصیص کدهای آزاد و سپس دسته‌بندی آن‌ها بر اساس اهداف تحقیق برای هر هدف انجام شده است. درنهایت در گام سوم، قضاوت و تصمیم‌گیری با توجه به شبکه‌ها و داده‌های استخراج شده از دسته‌بندی کدها و پس از پردازش جهت دستیابی و رسیدن به هدف مربوطه انجام گرفته است.

جهت بررسی پایایی ابزار سنجش در این پژوهش از آزمون آلفای کرونباخ که با استفاده از نرم‌افزار اسمارت پی‌ال‌اس به‌دست‌آمده استفاده شده است. نتایج این آزمون در شکل (۱) و جدول (۲) ارائه شده است.

<sup>۱</sup> Simple Random Sampling



شکل (۱) خروجی نرم‌افزار SMART PLS جهت محاسبه آلفای کرونباخ مؤلفه‌ها

جدول (۱) مقادیر آلفای کرونباخ و پایایی ترکیبی متغیر تحقیق و مؤلفه‌های آن

متغیر پژوهش	آلفا کرونباخ	پایایی مرکب	مؤلفه‌های پژوهش	آلفا کرونباخ	پایایی مرکب	مؤلفه‌های پژوهش	آلفا کرونباخ	پایایی مرکب
شبیه‌های نفوذ به محرمانگی در شبکه‌های اد هاک	۰/۹۰۳	۰/۹۱۶	حملات کلاسیک فعال	۰/۸۷۵	۰/۸۹۷	حملات کلاسیک	۰/۸۰۰	۰/۸۴۶
			حملات کلاسیک غیرفعال	۰/۸۲۵		حملات کلاسیک	۰/۸۳۵	۰/۸۷۰
			حملات کلاسیک بر اساس پایگاه مینر اتک	۰/۷۷۶	۰/۸۵۰			

جدول (۲): مقادیر بارهای عاملی گویه‌ها

مؤلفه تحقیق			گویه‌ها
حملات بر اساس پایگاه مینر اتک در حوزه محرمانگی	حملات کلاسیک غیرفعال در حوزه محرمانگی	حملات کلاسیک فعال در حوزه محرمانگی	

مؤلفه تحقیق			گویه‌ها
حملات بر اساس پایگاه میتر اتک در حوزه محرمانگی	حملات کلاسیک غیرفعال در حوزه محرمانگی	حملات کلاسیک فعال در حوزه محرمانگی	
		۰/۵۱۹	حمله انکار سرویس
		۰/۵۴۰	حمله کرم‌چاله
		۰/۶۲۵	حمله تزریق بسته
		۰/۵۶۲	حمله استهلاک منابع
		۰/۵۳۱	حمله نفوذ رله تبانی
		۰/۴۹۱	حمله جعل شبکه سلولی
		۰/۷۸۲	حمله بالماسکه کردن
		۰/۷۳۹	حمله بازپخش حمله
		۰/۷۳۰	حمله جعل هویت
	۰/۷۱۳		حمله استراق سمع
	۰/۴۳۴		حمله تجزیه و تحلیل ترافیک
	۰/۷۴۸		حمله مردمیانی غیرفعال
	۰/۸۱۱		حمله همبستگی ترافیک
	۰/۷۴۱		حمله استخراج بسته
	۰/۶۷۷		حمله ره‌گیری ترافیک
	۰/۷۴۴		حمله نشت اطلاعات
۰/۷۷۶			حمله جلوگیری از سرویس از راه دور
۰/۷۵۴			حمله کرک دلبیو پی‌ای / دلبیو پی‌ای دو
۰/۷۸۲			حمله به احراز هویت
۰/۷۶۳			حمله سازش بی‌سیم
۰/۵۵۳			حمله دوقلوهای شیطانی

شیوه محاسبه بار عاملی بدین‌صورت است که از طریق محاسبه با استفاده از نرم‌افزار اسمارت پی‌ال‌اس مقدار ارتباط هر یک از گویه‌های سازه با آن سازه محاسبه می‌گردد، چنانچه این مقدار برابر و یا بیشتر از مقدار ۰/۴ شود، مؤید این مطلب است که واریانس بین سازه و شاخص‌های آن از واریانس خطای اندازه‌گیری آن سازه بیشتر بوده و پایایی در مورد آن مدل اندازه‌گیری قابل‌قبول است. همان‌طور که در جدول (۳) قابل‌مشاهده است کلیه بارهای عاملی گویه‌های پژوهش بیشتر از ۰/۴ هستند که نشان‌دهنده پایایی قابل‌قبول مدل اندازه‌گیری دارد.

عامل دیگری که مورد محاسبه قرار گرفته است، عامل تورم واریانس<sup>۱</sup> است که شدت هم خطی چندگانه را در تحلیل رگرسیون کمترین مربعات معمولی ارزیابی می‌کند. به بیان ساده شاخص VIF نشان می‌دهد که یک متغیر تا چه اندازه تحت تأثیر دیگر متغیرها رفتارش تغییر می‌کند. شدت هم خطی چندگانه را با بررسی بزرگی مقدار VIF می‌توان تحلیل نمود. عامل تورم واریانس یا VIF از تقسیم عدد یک بر تلورانس حاصل می‌شود، هرچه مقدار عامل تورم واریانس از عدد ۲ بزرگ‌تر باشد میزان هم خطی بیش‌تر است. نتیجه و تفسیر عامل تورم واریانس، معکوس تلورانس است یعنی هر چه مقدار تلورانس بیش‌تر باشد، مقدار عامل تورم واریانس کم‌تر است و برعکس. به عبارتی هر چه مقدار این ضریب افزایش یابد باعث می‌شود که واریانس ضرایب رگرسیونی افزایش یافته و در نتیجه مدل رگرسیون را برای پیش‌بینی نامناسب جلوه می‌دهد؛ بنابراین هر چه مقدار عمل تورم واریانس برای یک متغیر مستقل بیش‌تر از عدد ۳ باشد نتیجه می‌گیریم که آن متغیر نقش زیادی در مدل، نسبت به بقیه تغییرها ندارد.

جدول (۳) شاخص تورش واریانس VIF بیرونی برای تمامی متغیرهای وارد شده

ردیف	حمله	VIF	ردیف	حمله	VIF
۱	حمله انکار سرویس	۱/۳۸۳	۱۲	حمله تجزیه و تحلیل ترافیک	۱/۷۷۵
۲	حمله کرم چاله	۱/۶۴۳	۱۳	حمله مردمیانی غیرفعال	۱/۸۸۸
۳	حمله تزریق بسته	۱/۳۶۶	۱۴	حمله همبستگی ترافیک	۲/۱۲۴
۴	حمله استهلاک منابع	۱/۴۰۸	۱۵	حمله استخراج بسته	۱/۸۳۶
۵	حمله نفوذ رله تبانی	۱/۳۴۲	۱۶	حمله ره‌گیری ترافیک	۱/۶۲۸
۶	حمله جعل شبکه سلولی	۱/۲۷۹	۱۷	حمله نشت اطلاعات	۱/۸۶۹
۷	حمله بالماسکه کردن	۱/۴۴۱	۱۸	حمله جلوگیری از سرویس از راه دور	۲/۷۸۰
۸	حمله بازپخش حمله	۲/۴۱۴	۱۹	حمله کرک دبلوی پی‌ای / دبلوی پی‌ای دو	۲/۳۹۵
۹	حمله جعل هویت	۲/۲۹۰	۲۰	حمله به احراز هویت	۱/۷۴۹
۱۰	حمله انکار سرویس	۱/۶۱۷	۲۱	حمله سازش بی‌سیم	۱/۵۴۶
۱۱	حمله استراق سمع	۲/۱۲۲	۲۲	حمله دوقلوهای شیطانی	۱/۳۱۸

<sup>۱</sup> Variance Inflation Factor (VIF)

## جدول (۴) شاخص تورش واریانس VIF درونی برای تمامی متغیرهای وارد شده

شیوه‌های نفوذ به محرمانگی در شبکه‌های اد هاک	
۲/۱۰۸	حملات بر اساس پایگاه داده میتر اتک در حوزه محرمانگی
۲/۱۰۸	حملات کلاسیک در حوزه محرمانگی

همان‌طور که از جداول (۴) و (۵) قابل مشاهده است VIF متغیرها و گویه‌های تحقیق نقش زیادی در مدل ارائه شده دارند و به عبارتی پایایی تحقیق را تأیید می‌نماید. سپس گویه‌های استخراج و با استفاده از نرم‌افزار اسمارت پی‌ال‌اس فرض‌های تحقیق مورد آزمون قرار گرفته است.

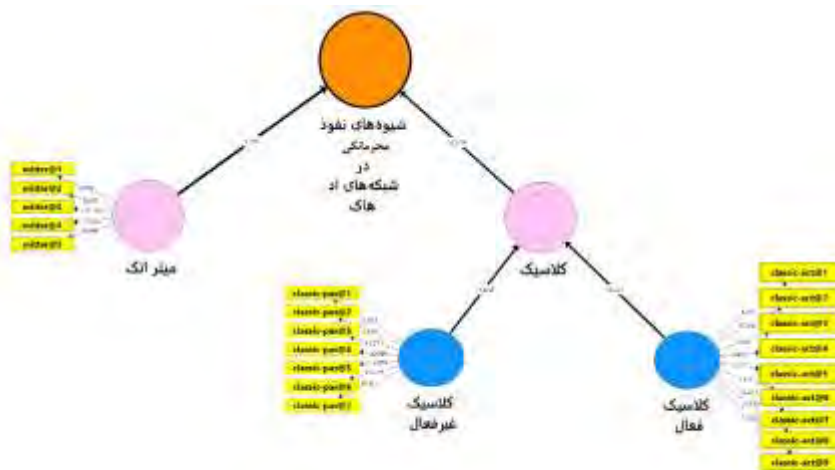
برای این که بتوانیم کیفیت و قابل قبول بودن مدل اندازه‌گیری را بیشتر مورد ارزیابی قرار دهیم با استفاده از مدل شاخص اندازه‌گیری (شاخص اشتراک) سنجیده شد، این شاخص توانایی مدل را در پیش‌بینی متغیرهای مشاهده‌پذیر از طریق مقادیر متغیر پنهان متناظرشان می‌سنجد. چنانچه مقادیر این شاخص مثبت باشند نشانگر آن است که مدل ارائه شده کیفیت مناسب و قابل قبول را دارد. در جدول (۶) می‌توان مقادیر این شاخص که مربوط به هر یک از متغیرها پژوهش است را مشاهده کرد. همان‌طور که مشاهده می‌شود کلیه مقادیر بزرگ‌تر از صفر و مثبت هستند؛ که نشان دهنده کیفیت مناسب و قابل قبول بودن مدل‌ها است.

## جدول (۵) نتایج آزمون کیفیت مدل اندازه‌گیری

CV.Com	متغیر
۰/۲۷۲	شیوه‌های نفوذ به محرمانگی در شبکه‌های اد هاک
۰/۳۰۲	حملات بر اساس پایگاه داده میتر اتک در حوزه محرمانگی
۰/۲۶۴	حملات کلاسیک در حوزه محرمانگی
۰/۳۳۳	حملات کلاسیک غیرفعال در حوزه محرمانگی
۰/۲۳۲	حملات کلاسیک فعال در حوزه محرمانگی

یافته‌های پژوهش (تحلیل‌های بخش کمی که با اس پی اس انجام شده کجاست؟) در جهت ارزیابی میزان برازش مدل ساختاری بر اساس ضرایب معناداری مقادیر t-values در نرم‌افزار اسمارت پی‌ال‌اس استفاده گردید که با اجرای فرمان بوت استرپینگ مقادیر بر روی خطوط مسیره‌ها نشان داده می‌شوند. برای تأیید فرضیه پژوهش می‌بایست مقادیر از  $1/96$  بیش‌تر باشد تا صحت رابطه بین سازه‌ها در سطح اطمینان ۹۵ درصد تأیید گردد. در شکل (۲) و جدول (۷) می‌توان مقادیر به‌دست‌آمده برای ارزیابی بخش ساختاری مدل را مشاهده نمود. کلیه مقادیر از عدد

ذکر شده بالاتر هستند که حاکی از معنادار بودن مسیرها، تأیید تمام فرضیه‌های پژوهش و مناسب بودن مدل ساختاری است.



شکل (۲) خروجی نرم‌افزار SMART PLS جهت محاسبه نتایج آزمون مسیر و آماره T

جدول (۶) نتایج آزمون مسیر و آماره T

مقادیر P	آماره T	انحراف استاندارد (STDEV)	میانگین نمونه (M)	ضریب مسیر	
۰/۰۰۰	۱۲/۴۱۸	۰/۰۳۰	۰/۳۷۱	۰/۳۷۰	حملات بر اساس پایگاه داده میترا تک در حوزه محرمانگی - شیوه‌های نفوذ به محرمانگی در شبکه‌های اد هاک
۰/۰۰۰	۲۱/۵۲۶	۰/۰۳۳	۰/۶۹۷	۰/۷۰۰	حملات کلاسیک در حوزه محرمانگی - شیوه‌های نفوذ به محرمانگی در شبکه‌های اد هاک
۰/۰۰۰	۱۱/۶۳۱	۰/۰۴۸	۰/۵۵۶	۰/۵۵۸	حملات کلاسیک غیر فعال در حوزه محرمانگی - حملات کلاسیک در حوزه محرمانگی
۰/۰۰۰	۱۰/۸۴۸	۰/۰۴۹	۰/۵۲۴	۰/۵۲۸	حملات کلاسیک فعال در حوزه محرمانگی - حملات کلاسیک در حوزه محرمانگی

با تأمل در موارد بیان شده و با توجه به اطلاعات استخراج شده در بند پردازش داده‌ها می‌توان بر اساس اسناد و مدارک مرتبط و مصاحبه با صاحب‌نظران چنین نتیجه گرفت که با در نظر گرفتن میزان تأکید بر نوع حملات به شبکه‌های اد\_هاک در حوزه محرمانگی، برمبنای حملات کلاسیک و میترا تک، شیوه‌های نفوذ به شرح زیر است:

با بهره‌برداری از آمار توصیفی و با توجه به جدول (۲) تا (۷) و با در نظر گرفتن بار عاملی هر کدام از گویه‌ها بر روی مؤلفه‌های و ابعاد پژوهش، هر شاخص از دیدگاه پاسخ‌دهندگان، شاخص‌های احصاء شده برای هر مؤلفه در بعد محرمانگی به شرح زیر است:

مؤلفه کلاسیک فعال شامل:

۱- حمله بالماسکه کردن - (۰/۷۸۲)

۲- حمله بازپخش حمله - (۰/۷۳۹)

۳- حمله جعل هویت - (۰/۷۳۰)

۴- حمله تزریق بسته - (۰/۶۲۵)

۵- حمله استهلاک منابع - (۰/۵۶۲)

۶- حمله کرم‌چاله - (۰/۵۴۰)

۷- حمله نفوذ رله تبانی - (۰/۵۳۱)

۸- حمله انکار سرویس - (۰/۵۱۹)

۹- حمله جعل شبکه سلولی - (۰/۴۹۱)

مؤلفه کلاسیک غیرفعال شامل:

۱- حمله استراق سمع - (۰/۸۱۱)

۲- حمله تجزیه و تحلیل ترافیک - (۰/۷۴۸)

۳- حمله مردمیانی غیرفعال - (۰/۷۴۴)

۴- حمله همبستگی ترافیک - (۰/۷۴۱)

۵- حمله استخراج بسته - (۰/۷۱۳)

۶- حمله ره‌گیری ترافیک - (۰/۶۷۷)

۷- حمله نشت اطلاعات - (۰/۴۳۴)

مؤلفه میتر اتک شامل:

۱- حمله جلوگیری از سرویس از راه دور - (۰/۷۷۶)

۲- حمله کرک دلیو پی‌ای / دلیو پی‌ای دو - (۰/۷۵۴)

۳- حمله به احراز هویت - (۰/۷۸۲)

۴- حمله سازش بی‌سیم - (۰/۷۶۳)

۵- حمله دوقلوهای شیطانی - (۰/۵۵۳)

از آنجا که شاخص‌های بعد محرمانگی بر اساس نظرات ارزشمند صاحب‌نظران و همچنین مطالعه و تجزیه و تحلیل اسناد و مدارک در مرحله تجزیه و تحلیل کیفی احصاء گردید و سپس نظرات



مورد تجزیه و تحلیل کیفی قرار گرفته و سپس بر اساس نتایج به دست آمده پرسشنامه تدوین، جهت پاسخگویی برای گروه نمونه ارسال و پس از جمع‌آوری با نرم‌افزار آماری اس.پی.اس.اس و اسمارت پی‌ال‌اس مورد تجزیه و تحلیل کمی (توصیفی) قرار گرفته که در جمع‌بندی کلی، نتایج نهایی بر اساس و سؤالات تحقیق به شرح زیر استخراج گردیده است.

با توجه به یافته‌های تحقیق می‌توان به شرح زیر نتیجه‌گیری نمود که موارد استفاده از شبکه‌های اد\_هاک به دلیل راحتی و سرعت در استقرار، تحرک بالا و همچنین توپولوژی پویای آن امروزه رو به افزایش است. از اماکنی که در آن استفاده از این شبکه در حال افزایش است می‌توان به سازمان‌های نظامی اشاره نمود که چند نمونه آن در بخش مبانی نظری اشاره گردید. شرکت هرمس به عنوان یک شرکت بزرگ ارائه‌دهنده بی‌سیم‌های نظامی با قابلیت بهره‌گیری از شبکه اد\_هاک است؛ در این پژوهش سعی شده است تا حداکثر دقت در انتخاب روش‌های نفوذ متناسب با شبکه اد\_هاک نظامی انجام گیرد و در این راه از منبع معتبر و نظر خبرگان استفاده شده که نتایج آن برای نفوذ به محرمانگی به شرح زیر آورده شده است.

محرمانگی همان‌طور که بیان شد، به محافظت از داده‌های ارسال شده توسط یک دستگاه اشاره دارد به طوری که توسط یک فرد یا نقطه دسترسی غیرمجاز، غیرقابل خواندن شود. از آنجایی که شبکه‌های بی‌سیم در تمام جهات منتشر می‌شوند و در محدوده انتقال مستقیم داده قرار دارند، بازیابی داده‌ها و شنود را ساده می‌کنند، بنابراین بسیار مهم است که داده‌ها از کاربر یا دستگاه غیرمجاز محرمانه نگه داشته شوند. در حال حاضر روش‌های بسیاری برای حفظ محرمانگی در شبکه‌های اد\_هاک مورد استفاده قرار می‌گیرد که نفوذ به آن را تا حدودی مشکل می‌نماید.

مهم‌ترین شیوه‌های نفوذ به شبکه‌های اد\_هاک در حوزه محرمانگی، بر اساس تجزیه و تحلیل انجام شده، عبارت‌اند از:

- حملات کلاسیک فعال، مشتمل بر حمله جعل هویت، حمله تزریق بسته، حمله سیبیل، حمله جعل شبکه سلولی و حمله انکار سرویس؛
- حملات کلاسیک غیرفعال مشتمل بر حمله تجزیه و تحلیل ترافیک، حمله ره‌گیری ترافیک، حمله استشمام بسته، حمله استخراج بسته و حمله نشت اطلاعات؛
- حملات میتر اتم مشتمل بر حمله جلوگیری از سرویس از راه دور و حمله کرک دبلو پی‌ای / دبلو پی‌ای دو.

#### پیشنهاد‌های اجرایی

۱- استفاده از پروتکل‌های امنیتی به‌روز نظیر دبلو پی‌ای ۳ در دستگاه‌هایی که بر مبنای شبکه‌های اد\_هاک فعالیت می‌کنند می‌تواند در بالا بردن امنیت آن‌ها کمک به سزایی نماید و

تا حدودی شبکه را در مقابله حملات جعل هویت، جلوگیری از حمله کرک دلیو پی ای/دلیو پی ای ۲ و حمله استخراج بسته ایمن نماید.

۲- پیش‌بینی سیستم تشخیص نفوذ در ساختار شبکه اد هاک به‌منظور پایش شبکه و شناسایی فعالیت غیرمجاز در جهت شناسایی حمله تزریق بسته و حمله نشت اطلاعات می‌تواند مورد استفاده قرار گیرد.

۳- تهیه پروتکل و الگوریتم‌های رمز بر پایه فناوری‌های داخلی در جهت جلوگیری از شنود در شبکه.

۴- تهیه بسته‌های امنیتی متفاوت جهت جلوگیری از ورود غیرمجاز کاربران به شبکه.

#### تشریح یافته‌های علمی تحقیق

نتایج حاصل از تحقیق نشان می‌دهد که شبکه‌های اد\_هاک در برابر حملات ذکر شده بیشتر از همه آسیب‌پذیر بوده و در جهت افزایش امنیت در شبکه اد هاک می‌بایست بیشترین تمرکز بر روی این حملات قرار گیرد.

#### قدردانی

از تمامی خبرگان و اساتیدی که دانش خویش را سخاوتمندانه در اختیار محققان این پژوهش قرار دادند، کمال تشکر را داریم.

#### منابع

≠ افشار هراتی، نسرین. (۱۴۰۰). بررسی ساختارهای امنیت در شبکه‌های Ad Hoc با رویکرد نو، پنجمین همایش بین‌المللی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران، تهران، <https://civilica.com/doc/1238055>.

≠ شاهسوندی، محمد. (۱۳۹۲). شبکه اد هاک، پایان‌نامه کارشناسی ارشد، مهندسی فناوری اطلاعات، دانشکده مهندسی، دانشگاه پیام نور واحد ایذه، ایذه.

≠ محمدی حمیدرضا. بررسی روش‌های نفوذ در شبکه‌های بی‌سیم Wi-Fi. امنیت فضای تولید و تبادل اطلاعات (منادی). (۱)۹: ۳۸-۳۱.

≠ Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile Ad Hoc routing protocols. 10(4), 78-93. doi:10.1109/SURV.2008.080407.

≠ Agrawal, R., Faujdar, N., Romero, C., Sharma, O., Abdulsahib, G., Khalaf, O., Ghoneim, O. (2023, March). Classification and comparison of ad hoc networks: A review. Egyptian Informatics Journal, 24(1), 1-25. doi:<https://doi.org/10.1016/j.eij.2022.10.004>.

≠ Barmanroy, D., & Chaki, R. (2014). Different Types of Attacks for WANs. In N. Chaki, & R. Chaki, *Intrusion Detection in Wireless Ad-Hoc Networks* (pp. 95-110).

- ≠ Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (2013). *Mobile Ad Hoc Networking: Cutting Edge Directions* (Second ed., Vol. 23).
- ≠ Chang, T.-H., Lin, J.-W., Chen, C.-M., & Lai, G.-H. (2018). The Method of Capturing the Encrypted Password Packets of WPA & WPA2, Automatic, Semi-Automatic or Manual? 2018 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-4). Kaohsiung, Taiwan: IEEE. doi:10.1109/DESEC.2018.8625156
- ≠ Copeland, M. (2021). *Cloud Defense Strategies with Azure Sentinel: Hands-on Threat Hunting in Cloud*. New Braunfels, TX, USA. doi:https://doi.org/10.1007/978-1-4842-7132-2.
- ≠ Enterprise Matrix. (2020, December 29). Retrieved from attack.mitre.org: https://attack.mitre.org/matrices/enterprise/ Enterprise Matrix.
- ≠ FM 3-0. (2017, October 6). *Operations*. Headquarters, Department Of The Army. Washington: Department of the Army USA.
- ≠ Harris Corporatio. (2024). AN/PRC-167 MULTI-CHANNEL MANPACK. Retrieved from www.l3harris.com: https://www.l3harris.com/all-capabilities/an-prc-167-multi-channel-manpack.
- ≠ Harris Corporation. (2024, January 13). AN/PRC-163 MULTI-CHANNEL HANDHELD RADIO. Retrieved from www.l3harris.com/: https://www.l3harris.com/all-capabilities/an-prc-163-multi-channel-handheld-radio.
- ≠ Nabben, K., & Rennie, E. (2022). Ad hoc network. *Internet Policy Review*, 11(2). Retrieved from https://doi.org/10.14763/2022.2.1666.
- ≠ Sbai, O., & Elboukhari, M. (2018). Classification of Mobile Ad Hoc Networks Attacks. *Chulalongkorn University provided by UniNet*, 618-624.
- ≠ Singh, J., Dutta, P., & Chakrabarti, A. (2018). *Ad Hoc Networks* (1 ed.). Springer Singapore. doi:https://doi.org/10.1007/978-981-10-8770-7.
- ≠ Stukova , I., & Crawford, B. (2019, Lune). Short-Term Self-Moving Tactical Networks In Austere Environments. *Master Of Science In Network Operations And Technology*, 123. Monterey, California.
- ≠ Toh, C., Lee, E., & Ramos, N. (2004). Next-generation tactical ad hoc mobile wireless. *Technology Review Journal*, 125.